

2/5/1 (Item 1 from file: 351)
DIALOG(R) File 351:Derwent WPI
(c) 2002 Derwent Info Ltd. All rts. reserv.

011490013 **Image available**
WPI Acc No: 1997-467918/ 199743
XRPX Acc No: N97-390315

Electronic shopping method for retail store - by subtracting price of goods, ordered and delivered to buyer from retail store, by credit card company after confirming validity of authentication information produced by buyer and porter

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 9218896	A	19970819	JP 9622783	A	19960208	199743 B

Priority Applications (No Type Date): JP 9622783 A 19960208

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9218896	A		11	G06F-017/60	

Abstract (Basic): JP 9218896 A

The method involves producing the authentication information relating to a goods order sheet by a buyer during the order of goods. The authentication information and goods order sheet are transmitted to a retail store. The retail store confirms the validity of the authentication information from the buyer. Ordered goods of the buyer are passed to a porter and shipped by the personnel in the retail store after verifying the authentication information from the buyer.

When the buyer receives the ordered goods, the buyer demands for the goods receipt document and the porter confirms the validity of the authentication information in a duplicate copy. The goods receipt document and the confirmed authentication information in the duplicate copy are send by the retail store to a credit card company. The credit card company subtracts the price of ordered goods from the bank account of the buyer after confirming the validity of the authentication information from the buyer and porter.

ADVANTAGE - Prevents reduction of price of ordered goods from buyer bank account without passing goods. Safely transfers information until protected goods corresponding to buyer order is delivered.

Dwg.1/8

Title Terms: ELECTRONIC; SHOPPING; METHOD; RETAIL; STORAGE; SUBTRACT; PRICE ; GOODS; ORDER; DELIVER; BUY; RETAIL; STORAGE; CREDIT; CARD; COMPANY; AFTER; CONFIRM; VALID; AUTHENTICITY; INFORMATION; PRODUCE; BUY; PORTER

Derwent Class: P85; T01; T05; W01

International Patent Class (Main): G06F-017/60

International Patent Class (Additional): G09C-001/00; H04L-009/32

File Segment: EPI; EngPI

2/5/2 (Item 1 from file: 347)
DIALOG(R) File 347:JAPIO
(c) 2002 JPO & JAPIO. All rts. reserv.

05604096 **Image available**
ELECTRONIC SHOPPING METHOD AND DEVICE

PUB. NO.: 09-218896 [JP 9218896 A]
PUBLISHED: August 19, 1997 (19970819)
INVENTOR(s): NISHIOKA GENJI
SASAKI RYOICHI
SUZAKI SEIICHI
UMEKI HISASHI
HANAOKA KAHORU

APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP
(Japan)
APPL. NO.: 08-022783 [JP 9622783]
FILED: February 08, 1996 (19960208)
INTL CLASS: [6] G06F-017/60; G09C-001/00; G09C-001/00; H04L-009/32
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 44.3
(COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)
JAPIO KEYWORD: R139 (INFORMATION PROCESSING -- Word Processors)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method for preventing illegality that a dishonest retail shop withdraws the information of a credit card from a purchaser and obtains a charge without delivering a product to the purchaser and making the purchaser safely recognize the carrying conditions of the product ordered by himself/ herself.

SOLUTION: The purchaser prepares authentication information in ordering the product and in receiving the product and a credit card company withdraws a product charge from the bank account of the purchaser after confirming the propriety of both of the authentication information. Also, the retail shop 300 arbitrarily prepares a ciphering key and a deciphering key intrinsic to the product in shipping the product ordered by the purchaser and delivers them respectively to a carrier 500 and the purchaser 200, the carrier 500 ciphers the information of the carrying conditions of the product by the ciphering key and stores it in a reliable server 700 and the purchaser 200 accesses the server 700 and views the carrying conditions of the product by using the deciphering key.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-218896

(43) 公開日 平成9年(1997)8月19日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21	3 4 0 A
G 0 9 C 1/00	6 4 0	7259-5 J	G 0 9 C 1/00	6 4 0 B
	6 6 0	7259-5 J		6 6 0 B
		7259-5 J		6 6 0 G
H 0 4 L 9/32			G 0 6 F 15/21	Z

審査請求 未請求 請求項の数 7 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願平8-22783

(22) 出願日 平成8年(1996)2月8日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 西岡 玄次

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 佐々木 良一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

最終頁に続く

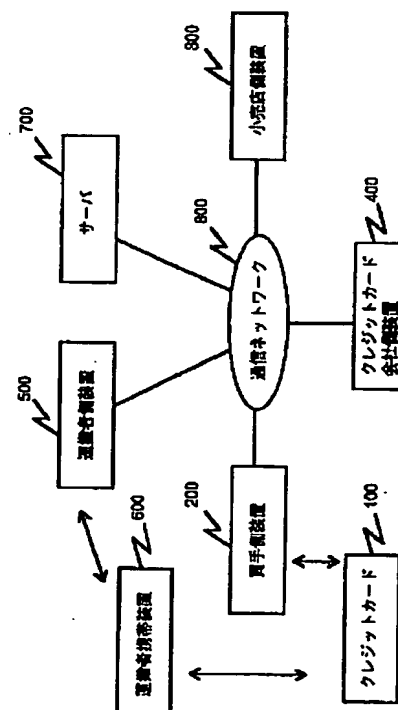
(54) 【発明の名称】 電子ショッピング方法および装置

(57) 【要約】

【課題】電子ショッピングシステムにおいて、不正な小売店が買手からクレジットカード100の情報を引き出し、商品を買手に渡すことなく代金を得る不正を防止し、かつ、買手が自分の発注した商品の運搬状況を安全に知る方法を提供する。

【解決手段】買手は商品発注時と商品受け取り時に認証情報を作成し、クレジットカード会社は双方の認証情報の正当性を確かめた上で、買手の銀行口座から商品代金を引き落とす。また、小売店は買手の注文商品の発送時に商品固有の暗号化鍵と復号化鍵を任意に作成し、それぞれを運搬者および買手に渡し、運搬者は商品の運搬状況の情報を暗号化鍵で暗号化して信頼できるサーバ700に格納し、買手はサーバ700にアクセスし、復号化鍵を用いて商品の運搬状況を見る。

システム構成 (図1)



【特許請求の範囲】

【請求項1】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手は商品注文時に商品注文書Pに関する認証情報I1を作成し、PとI1を小売店に送り、

小売店は認証情報I1の正当性を確かめた後、買手の注文した該商品を運搬者に渡し発送し、さらにPとI1をクレジットカード会社に送り、

買手は運搬者から該商品を受け取った際に、商品受取書Rに対して認証情報I2を作成し、I2を運搬者に渡し、

運搬者はI2の正当性を確かめた後、RとI2を（小売店経由で）クレジットカード会社に送信し、クレジットカード会社はI1とI2の正当性を確かめた後、該商品代金を買手の銀行口座から引き落とすことを特徴とする電子ショッピング方法。

【請求項2】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手のクレジットカードには買手固有の秘密鍵dと公開鍵(e, n)が搭載されており、クレジットカード会社は公開鍵(e, n)を管理しており、

買手は、商品注文時に商品注文書Pに対してクレジットカード内の秘密鍵dを用いて署名S1を、

$S1 = \exp(h(P), d) \mod n$,

にて作成し、PとS1を小売店に送り、

小売店は、クレジットカード会社に買手の公開鍵(e, n)を問い合わせ、

$h(P) \exp(S1, e) \mod n$,

を確かめることにより署名S1の認証を行った後、買手の注文した該商品を運搬者に渡し発送し、さらにPとS1をクレジットカード会社に送信し、

買手は運搬者から該商品を受け取った際に、クレジットカード内の秘密鍵dを用いて商品受取書Rに対して、

$S2 = \exp(h(R), d) \mod n$,

にて、署名S2を作成し、S2を運搬者に渡し、

運搬者は、買手のクレジットカードから出力された公開鍵(e, n)を用いて、

$h(R) \exp(S2, e) \mod n$,

を確かめることにより署名S2の認証を行った後、RとS2を（小売店経由で）クレジットカード会社に送信し、

クレジットカード会社は、クレジットカード会社に保管

されている買手の公開鍵(e, n)を用いて、

$h(P) \exp(S1, e) \mod n$,

$h(R) \exp(S2, e) \mod n$,

を確かめることにより、S1とS2の認証を行った後、該商品代金を買手の銀行口座から引き落とすことを特徴とする電子ショッピング方法。ただし、 $n = pq$ (p, qは素数), $ed \equiv 1 \mod N$ (Nは $p-1$ と $q-1$ の最小公倍数)であり、 $\exp(a, x)$ はaをx乗した値を表し、hは公開されたハッシュ関数を表す。

10 【請求項3】請求項1および請求項2において、商品受取書および受取書に対する買手の署名のコピーのデータを買手のクレジットカードまたは他の記憶媒体に記録し、買手は該データを保管することを特徴とする電子ショッピング方法。

20 【請求項4】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

小売店は買手の注文した商品発送時に該商品に対して識別情報Iと固有の鍵情報（暗号化鍵と復号化鍵）を設定し、小売店は識別情報Iと該復号化鍵を買手に送信し、買手の注文した該商品と識別情報Iと該暗号化鍵を運搬者に渡し、

運搬者は該商品の運搬状況の情報を該暗号化鍵で暗号化した暗号化データを信頼できるサーバに格納し、

買手は該商品の運搬状況を知ることを目的に該サーバにアクセスし、該商品の識別情報Iから該暗号化データを検索し、該暗号化データを該復号化鍵で復号化することを特徴とする電子ショッピング方法。

30 【請求項5】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手のクレジットカードには買手固有の秘密鍵dと公開鍵(e, n)が搭載されており、クレジットカード会社は公開鍵(e, n)を管理しており、

買手は、商品注文時に商品注文書Pに対してクレジットカード内の秘密鍵dを用いて署名S1を、

$S1 = \exp(h(P), d) \mod n$,

にて作成し、PとS1を小売店に送り、

小売店は、クレジットカード会社に買手の公開鍵(e, n)を問い合わせ、

$h(P) \exp(S1, e) \mod n$,

を確かめることにより署名S1の認証を行った後、買手からの該注文商品に対して識別情報Iと固有の鍵情報K（共通鍵暗号の鍵）を設定し、小売店は該商品と識別情

報Iと鍵情報Kを運搬者に渡し、さらに買手の公開鍵
(e, n)を用いて、
 $W = \exp(K, e) \mod n$,
 にて鍵Kを暗号化して、WとIを買手に送信し、
 運搬者は該商品の運搬状況の情報Sを鍵Kで、
 $E = E(S : K)$,
 にて暗号化して、信頼できるサーバに格納し、
 買手は小売店から送られてきた暗号文Wから、クレジット
 カード内の秘密鍵dと公開鍵(e, n)を用いて、
 $K = \exp(W, d) \mod n$,
 にて、鍵Kを復号化し、さらに該商品の運搬状況を知る
 ことを目的に該サーバにアクセスし、該商品の識別情報
 Iから該暗号化データEを検索し、鍵Kを用いて、
 $S = D(E : K)$,
 にて、Sを復号化することを特徴とする電子ショッピング
 方法。ただし、 $n = pq$ (p, qは素数), $ed \equiv 1$
 $(\mod N)$ (Nはp-1とq-1の最小公倍数)で
 あり、 $\exp(a, x)$ はaをx乗した値を表し、hは
 公開されたハッシュ関数を表わし、 $E(P : K)$, D
 $(P : K)$ はそれぞれ文書Pを鍵Kで暗号化、復号化し
 た結果を表す。

【請求項6】請求項2から請求項6のいずれかにおい
 て、
 クレジットカード会社は、買手の手元に商品が届けられ
 た日時から商品返品有効期間を経た後、買手の銀行口座
 から代金を引き落とすことを特徴とする電子ショッピング
 方法。

【請求項7】請求項1または2において、買手が商品受
 け取り時に受取書に対して署名を作成するときに用いら
 れる運搬者が所持する携帯可能な装置であって、
 受取書を表示する表示手段と、買手がクレジットカード
 内の秘密鍵を用いて作成した署名文を記憶する記憶手段
 と、該署名の正当性を確かめる検証手段を備えたことを
 特徴とする携帯可能な装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、買手が通信ネット
 ワークを介して商品発注を行う電子ショッピングシステム
 に関する。

【0002】

【従来の技術】一般にクレジットカードを用いて通信販
 売を行う場合、買手は商品発注の際に買手のクレジット
 カードの会社名、クレジットカード番号、有効期限、等
 の情報を小売店に知らせ、小売店はクレジットカード会
 社に対して代金請求を行ない、クレジット会社は後日買
 手の銀行口座から商品の代金引き落としを行っている。

【0003】

【発明が解決しようとする課題】しかし、この方法だ
 と、不正な小売店が買手からクレジットカードの情報を
 引き出し、商品発送を行わないで代金のみを得るような

不正が考えられる。

【0004】また、今日、インターネットを利用して、
 海外の通販業者に対して手軽にメールオーダーを行える
 ようになりつつある。しかし、国内と違って、買手の手
 元に商品が届くまでには相当の日数がかかり、買手は自
 分が注文した商品の状況（商品が現在どこにあって、い
 つ買手の手元に届くか等）が分かると便利である。

【0005】そこで、本発明の主目的は、(1)不正な
 小売店が買手からクレジットカードの情報を引き出し、
 10 商品を買手に渡すことなく代金を得る不正を防止する、
 (2)買手は、自分の発注した商品が買手の手元に届く
 までの運送状況を買手のプライバシーを保護し安全に知
 ることができる、という特徴を有する電子ショッピング
 システムを提供するものである。

【0006】

【課題を解決するための手段】上記目的(1)を達成す
 るために、本発明は、買手が商品発注時に作成した認証
 情報と商品受け取り時に作成した認証情報の双方の正当
 性を確かめた上で、クレジットカード会社は買手の銀行
 20 口座から代金を引き落とすようにしたことを特徴とす
 る。

【0007】具体的には、買手のクレジットカードには
 買手固有の秘密鍵dと公開鍵(e, n)が搭載されてお
 り、クレジットカード会社は公開鍵(e, n)を管理し
 ており、買手は、商品注文時に商品注文書Pに対してク
 レジットカード内の秘密鍵dを用いて署名S1を、
 $S1 = \exp(h(P), d) \mod n$,
 にて作成し、PとS1を小売店に送る。

【0008】小売店は、クレジットカード会社を買手の
 30 公開鍵(e, n)を問い合わせ、
 $h(P) \cdot \exp(S1, e) \mod n$,
 を確かめることにより署名S1の認証を行った後、買手
 の注文した商品を運搬者に渡し発送し、さらにPとS1
 をクレジットカード会社へ送信する。

【0009】買手は運搬者から商品を受け取った際に、
 クレジットカード内の秘密鍵dを用いて商品受取書Rに
 対して、

$S2 = \exp(h(R), d) \mod n$,

にて、署名S2を作成し、S2を運搬者に渡す。

40 【0010】運搬者は、買手のクレジットカードから出
 力された公開鍵(e, n)を用いて、
 $h(R) \cdot \exp(S2, e) \mod n$,
 を確かめることにより署名S2の認証を行った後、Rと
 S2を(小売店経由で)クレジットカード会社へ送信す
 る。

【0011】クレジットカード会社は、クレジットカード
 50 会社へ保管されている買手の公開鍵(e, n)を用い
 て、

$h(P) \cdot \exp(S1, e) \mod n$,

$h(R) \cdot \exp(S2, e) \mod n$,

を確かめることにより、S1とS2の認証を行った後、該商品代金を買手の銀行口座から引き落とす。ただし、 $n=pq$ (p, q は素数), $ed \equiv 1 \pmod{N}$ (N は $p-1$ と $q-1$ の最小公倍数)であり、 $\exp(a, x)$ は a を x 乗した値を表し、 h は公開されたハッシュ関数を表す。

【0012】また、上記目的(1)、(2)を達成するために、本発明は、小売店が注文商品を発送する際に作成した商品固有の暗号化鍵と復号化鍵をそれぞれ運搬者と買手に渡し、運搬者は買手の注文した商品の運搬状況の情報を暗号化鍵で暗号化して信頼できるサーバに格納し、買手はサーバにアクセスし、復号化鍵を用いて運搬状況の情報を復号化して、自分の注文した商品の運搬状況を知る。

【0013】具体的には、買手のクレジットカードには買手固有の秘密鍵 d と公開鍵 (e, n) が搭載されており、クレジットカード会社は公開鍵 (e, n) を管理しており、買手は、商品注文時に商品注文書 P に対してクレジットカード内の秘密鍵 d を用いて署名 $S1$ を、 $S1 = \exp(h(P), d) \pmod{n}$,
にて作成し、 P と $S1$ を小売店に送る。

【0014】小売店は、クレジットカード会社を買手の公開鍵 (e, n) を問い合わせ、 $h(P) \cdot \exp(S1, e) \pmod{n}$,
を確かめることにより署名 $S1$ の認証を行った後、買手からの注文商品に対して識別情報 I と固有の鍵情報 K (共通鍵暗号の鍵)を設定し、小売店は商品と識別情報 I と鍵情報 K を運搬者に渡し、さらに買手の公開鍵 (e, n) を用いて、 $W = \exp(K, e) \pmod{n}$,
にて鍵 K を暗号化して、 W と I を買手に送信する。

【0015】運搬者は商品の運搬状況の情報 S を鍵 K で、 $E = E(S : K)$,
にて暗号化して、信頼できるサーバに格納する。

【0016】買手は小売店から送られてきた W から、クレジットカード内の秘密鍵 d と公開鍵 (e, n) を用いて、 $K = \exp(W, d) \pmod{n}$,
にて、鍵 K を復号化し、さらに該商品の運搬状況を知ることが目的に該サーバにアクセスし、該商品の識別情報 I から該暗号化データ E を検索し、鍵 K を用いて、 $S = D(E : K)$,
にて、 S を復号化する。ただし、 $n=pq$ (p, q は素数), $ed \equiv 1 \pmod{N}$ (N は $p-1$ と $q-1$ の最小公倍数)であり、 $\exp(a, x)$ は a を x 乗した値を表し、 h は公開されたハッシュ関数を表わし、 $E = E(S : K)$, $D = D(E : K)$ はそれぞれ文書 P を鍵 K で暗号化、復号化した結果を表す。

【0017】なお、共通鍵を用いる暗号方式では、暗号

化鍵と復号化鍵が同一で、それぞれを秘密に管理する必要がある。これに対して、公開鍵暗号方式は、暗号化鍵と復号化鍵とが相異なっており、暗号化鍵は公開し、復号化鍵は秘密にする。これにより、誰でも暗号文をつくることができ、復号化鍵を持つ者だけが復号を行える。このことから、公開鍵暗号方式では暗号化鍵のことを公開鍵と呼び、復号化鍵を秘密鍵と呼ぶ。但し、デジタル署名においては、秘密鍵を用いて署名作成を行い、公開鍵を用いて署名検証を行う。すなわち、署名鍵を知る者のみ署名を作成でき、その署名が正当なものであるかどうかは誰でもが確かめることができるようにするものである。

【0018】ハッシュ関数とは、データを圧縮する関数であり、従来提案されているハッシュ関数(例えばMD2, MD5等)のうち適当なものを使用すればよい。圧縮されたデータが元に復元できなくてもよい。なお、ハッシュ関数の詳細については、例えば、岡本栄司著、「暗号理論入門」、共立出版(1993)、第138～141頁に記載されている。

【0019】また、公開鍵暗号については、前述の「暗号理論入門」の第88～91頁に記載されている。

【0020】本発明に係る電子ショッピング方法によれば、クレジットカード会社は商品発注時の署名と商品受け取り時の署名の双方の正当性を確かめた後、買手の銀行口座より代金を引き落とす。このため、不正な小売店が商品を発送せずに代金のみを得る不正を防止することができる。また、買手の注文した商品の運搬状況の情報を暗号化して信頼できるサーバに格納しているため、不正な小売店が商品発送を行わなかった場合、買手はこれを検出することができ、さらに第三者から買手のプライバシーを保護し、買手は商品が手元に届くまでの運搬状況の情報を得ることができる。

【0021】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態について詳しく説明する。

【0022】図1は、本発明の実施の形態1及び2のシステム構成を示す図である。このシステムは、クレジットカード100と買手側装置200と小売店側装置300とクレジットカード会社側装置400と運搬者側装置500と運搬者携帯装置600とサーバ700から構成されている。これらは、いずれもコンピュータにより実現される。買手側装置200と小売店側装置300とクレジットカード会社側装置400と運搬者側装置500とサーバ700は通信ネットワーク800を介して接続されている。運搬者携帯装置600および買手側装置200は、後述するように、クレジットカード100とのインタフェースを有する。

【0.0.2.3】図2はクレジットカード100の内部構成を示す。クレジットカード100は、メモリ101、署名作成装置102、暗復号化装置(公開鍵暗号)10

10

20

30

40

50

3、を備えている。

【0024】図3は買手側装置200の内部構成を示す。買手側装置200は、クレジットカード読み取り装置201、文書作成装置202、ハッシュ計算装置203、暗復号化装置（共通鍵暗号）204、メモリ205、通信装置206、を備えている。

【0025】図4は小売店側装置300の内部構成を示す。小売店側装置300は、ハッシュ計算装置301、署名検証装置302、暗復号化装置（公開鍵暗号）303、鍵生成装置304、通信装置305、を備えている。

【0026】図5はクレジットカード会社側装置400の内部構成を示す。クレジットカード会社側装置400は、署名検証装置401、メモリ402、を備えている。

【0027】図6は運搬者側装置500の内部構成を示す。運搬者側装置500は、メモリ501、通信装置502、暗復号化装置（共通鍵暗号）503、を備えている。

【0028】図7は、運搬者携帯装置600の内部構成を示す。運搬者携帯装置600は、クレジットカード読み取り装置601、ハッシュ計算装置602、署名検証装置603、メモリ604、通信装置605、表示装置606、を備えている。

【0029】買手は、クレジットカード100による代金精算を前提として小売店側装置300に商品発注を行い、運搬者を介して商品が買手のもとに配送される。

【0030】（実施の形態1）買手は商品発注時と商品受け取り時に認証情報を作成し、クレジットカード会社はそれらの正当性を認証した後、買手の銀行口座から代金を引き落とす。本実施の形態では、このような場合について以下に詳しく述べる。また、本実施の形態では、公開鍵暗号にRSA（前述の「暗号理論入門」の第88～91頁参照）を用いる。

【0031】買手はクレジットカード会社が発行したクレジットカード100を所持する。クレジットカード100内のメモリ101には買手固有の秘密鍵 d と公開鍵 (e, n) が格納されている。クレジットカード会社はクレジットカード側装置400内のメモリ402に買手の公開鍵 (e, n) を保管している。ただし、 $n = pq$ （ p, q は素数）、 $ed \equiv 1 \pmod{N}$ （ N は $p-1$ と $q-1$ の最小公倍数）。 $ed \equiv 1 \pmod{N}$ は、 $ed-1$ が N で割り切れることを意味する。

【0032】図8を参照しながら、本実施の形態におけるショッピングの流れを説明する。

【0033】（1）買手は購入を希望する商品を選び、買手側装置200内の文書作成装置202を用いて注文書 P （買手のID情報を含む）を作成する（81）。注文書は、各小売店が定めるものであり、通常、買物注文の日付、注文商品とその個数、合計金額、クレジットワ

ード会社名、クレジットカード番号、クレジットカードの有効期限等を記載したものである。さらに、買手はクレジットカード100を買手側装置200のクレジットカード読み取り装置201に接続する。買手側装置200はハッシュ計算装置203を用いて注文書 P のハッシュ値 $h(P)$ を計算し、クレジットカード100のメモリ101に出力する。クレジットカード100内は、メモリ101にある秘密鍵 d と署名作成装置102を用いてクレジットカード100内部にて、注文書 P に対する署名文 $S1$ を、

$$S1 = \exp(h(P), d) \pmod{n},$$

にて作成する（82）。この式は、 $S1 = \exp(h(P), d) \pmod{n}$ は、 $\exp(h(P), d)$ を n で割った余りを $S1$ とする、という意味である。ただし、 h は公開されたハッシュ関数で、 $\exp(a, x)$ は a を x 乗した値を表す。本例ではデジタル署名にRSAを用いているので、ハッシュ値 $h(P)$ は、 $0 \leq h(P) \leq n$ であればよい。クレジットカード100は、署名文 $S1$ を買手側装置200に出力する。買手側装置通信装置206を用いて注文書 P および署名文 $S1$ を小売店側装置300に通信ネットワーク800を介して送る（83）。なお、安全性の観点から n には512ビット以上の値が推奨される。

【0034】（2）小売店は、注文書 P および署名文 $S1$ を受け取ると、注文書 P に記載の買手のID情報を用いて、クレジットカード会社側装置400のメモリ402に格納されている買手の公開鍵 (e, n) を問い合わせる（84）。クレジット会社側装置400は、これに応答して公開鍵を返送する（85）。小売店側装置300は、公開鍵 (e, n) を受け取り、ハッシュ計算装置301と署名検証装置302を用いて、 $h(P) \equiv \exp(S1, e) \pmod{n}$ の成立を確かめる（86）。この式は、 $h(P) - \exp(S1, e)$ が n で割り切れることを意味する。これにより、署名文 $S1$ の認証を行う。

【0035】（3）小売店は、買手の注文した商品の発送を運搬者を通して行う（87）。また、代金の請求をクレジットカード会社に対して行う（88）。この際、注文書 P と署名文 $S1$ をクレジットカード会社へ送信する。

【0036】（4）買手は運搬者からの商品受け渡し時に、クレジットカード100を運搬者が携帯する運搬者携帯装置600のクレジットカード読み取り装置601に接続する。運搬者携帯装置600はハッシュ計算装置602を用いて商品受取書 R のハッシュ値 $h(R)$ を計算し、クレジットカード100に出力する（90）。商品受取書 R は、通常、運送業者が定めるものであり、発注者の名称、受取者の名称、日付等が記載されたものである。商品受取書 R は、通常、運搬者が小売店から商品発送を請け負った後に作成する。但し、小売店が作成

し、運搬者に商品発送を行った際に運搬車に渡すようにすることも可能である。クレジットカード100はメモリ101に格納された秘密鍵 d と署名作成装置102を用いて商品受取書 R に署名文 $S2$ をクレジットカード100内部で、

$$S2 = \exp(h(R), d) \pmod{n},$$

にて作成し、署名文 $S2$ と公開鍵 (e, n) を運搬者携帯装置600のメモリ604に出力する(90)。このとき、受取書 R および署名 $S2$ のコピーをクレジットカード100または他の記憶媒体に出力し、買手はこれを保管する、(5)運搬者携帯装置600は、署名検証装置603を用いて、

$$h(R) \equiv \exp(S2, e) \pmod{n},$$

を確かめることにより、署名文 $S2$ の認証を行った後、 $S2$ を運搬者側装置500のメモリ501に出力する

(91)。運搬者側装置500は通信装置502を用いて通信ネットワーク800を介して R と $S2$ をクレジットカード会社側装置400に送信する(92)。

【0037】(6)クレジットカード会社側装置400は、メモリ402に保管された買手の公開鍵 (e, n) と署名検証装置401を用いて、

$$h(P) \equiv \exp(S1, e) \pmod{n},$$

$$h(R) \equiv \exp(S2, e) \pmod{n},$$

を確かめることにより、 $S1$ と $S2$ の認証を行なう(93)。その後、商品受取書 R の日付情報から商品返品有効期間を経た後、クレジットカード会社は買手の銀行口座から商品の代金を引き落とす(94)。

【0038】以上、一般的な変数により説明したが、きわめて簡略化したRSAの一例を次に挙げる。

【0039】公開鍵： $n=55$, $e=7$

秘密鍵： $p=5$, $q=11$, $d=23$, $7 \times 23 = 1 \pmod{1 \text{ cm}(p-1, q-1) = 20}$,
ここに、 1 cm は最小公倍数を表す。

【0040】平文： $M=3$

暗号化： $C = \exp(M, e) \pmod{n}$,
 $\exp(M, e) = 3$ の7乗、 $n=55$ なので、 $C=42$ となる。

【0041】

復号化： $M = \exp(C, d) \pmod{n}$,

$\exp(C, d) = 42$ の23乗、 $n=55$ なので、 $M=3$ となる。

【0042】(実施の形態2)本実施の形態では、運送者は買手の注文商品の運搬状況の情報を信頼できるサーバに登録する。このような場合について、以下に詳しく述べる。また、本実施の形態においても、公開鍵暗号にRSAを用いる。

【0043】買手はクレジットカード会社が発行したクレジットカード100を所持し、クレジットカード100内のメモリ101には買手固有の秘密鍵 d と公開鍵 (e, n) が格納されており、クレジットカード会社は

クレジットカード側装置400内のメモリ402に買手の公開鍵 (e, n) を保管している。ただし、 $n=pq$ (p, q は素数), $ed \equiv 1 \pmod{N}$ (N は $p-1$ と $q-1$ の最小公倍数)。

【0044】(1)買手は購入を希望する商品を選び、買手側装置200内の文書作成装置202を用いて注文書 P (買手のID情報を含む)を作成する。さらに、買手はクレジットカード100を買手側装置のクレジットカード読み取り装置201に接続する。買手側装置200はハッシュ計算装置203を用いて注文書 P のハッシュ値 $h(P)$ を計算し、クレジットカード100に出力する。クレジットカード100内はメモリ101にある秘密鍵 d と署名作成装置102を用いてクレジットカード100内部にて、注文書 P に対する署名文 $S1$ を、
 $S1 = \exp(h(P), d) \pmod{n}$,
にて作成する。クレジットカード100は、署名文 $S1$ を買手側装置200に出力し、通信装置206を用いて注文書 P および署名文 $S1$ を小売店側装置300に通信ネットワーク800を介して送る。ただし、 h は公開されたハッシュ関数で、 $\exp(a, x)$ は a を x 乗した値を表す。

【0045】(2)小売店は、注文書 P に記載の買手のID情報を用いて、クレジットカード会社側装置400のメモリ402に格納されている買手の公開鍵 (e, n) を問い合わせる。小売店側装置300は、ハッシュ計算装置301と署名検証装置302を用いて、
 $h(P) \equiv \exp(S1, e) \pmod{n}$,
を確かめることにより、署名文 $S1$ の認証を行う。

【0046】(3)小売店は買手の注文商品に対してID番号 I を付け、さらに鍵生成装置304を用いて固有の鍵情報 K (共通鍵暗号の鍵)を作成する。小売店側装置300は暗復号化装置303を用いて鍵 K を買手の公開鍵 (e, n) から、
 $W = \exp(K, e) \pmod{n}$,
にて暗号化して、通信装置305を用いて I と W を通信ネットワーク800を介して買手側装置200に送る。さらに小売店は買手が注文した商品とID番号 I と鍵 K を運送業者に渡し、代金の請求をクレジットカード会社に対して行う。

【0047】(4)運送業者は商品の運搬状況 (商品がどこにあって、いつ買手の手元に到着するか等)を示す運搬状況の情報 S を逐次、運搬者側装置500内の暗復号化装置503を用いて S を鍵 K で暗号化する。すなわち、暗号文

$$E(S) = E(S : K),$$

を計算して、通信装置502を用いて通信ネットワーク800を介して信頼できるサーバ700に S を登録する。なお、共通鍵暗号方式としては、DES, FEAL等の公知のものを用いることができる。

【0048】(4)買手はクレジットカード100を買

手側装置200のクレジットカード読み取り装置201に接続し、Wをクレジットカード100に出力し、メモリ101内の秘密鍵dと暗復号化装置103を用いて、 $K = \exp(W, d) \bmod n$,
にて、鍵Kを復号化し、買手側装置200のメモリ205に出力する。買手は、買手の注文した商品の運搬状況を知ることを目的に買手側装置200内の通信装置206を用いてサーバ700にアクセスし、商品の識別情報Iから暗号化データE(S)を検索し、E(S)をメモリ205に格納する。買手側装置200は鍵Kと暗復号化装置204を用いて、
 $S = D(E : K)$,
にて、Sを復号化する。

【0049】(実施の形態3) 実施の形態1において、運搬者携帯装置600は文書を表示する表示装置606を備えており、買手は表示装置606に表示された商品受取書を視覚にて確認し、クレジットカード100を運搬者携帯装置600のクレジットカード読み取り装置601に接続し、実施の形態1の方法により署名を行う。さらに、運搬者携帯装置600は表示装置606に該署名の正否を表示する。表示装置606の画面に表示する内容としては、運搬内容、受取者名、差出名、運搬者名、受取日付、署名(済または未済)等が考えられる。署名の項目は、署名の正当性が確認されると「済」が表示される。

【0050】

【発明の効果】本発明によれば、買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピングシステムにおいて、クレジットカード会社は、買手の商品注文時のデジタル署名と商品受け取り時のデジタル署名の双方の正当性を確認した後、代金引き落としを行うため、不正な小売店が買手からクレジットカードの情報を引き出し、商品を買手に渡すことなく代金を得る不正を防止することができる。また、商品の運搬状況の情報を買手、小売店、および運搬者以外のものが知ることのできない鍵で暗号化してサーバに格納することにより、買手のプライバシーを保護しながら、買手は自分の発注した商品が買手の手元に届くまでの運送状況の情報を安全に知ることができる。

【図面の簡単な説明】

【図1】本発明のシステム構成を示す図である。

【図2】図1のシステム構成内のクレジットカードの内部構成を示す図である。

【図3】図1のシステム構成内の買手側装置の内部構成を示す図である。

【図4】図1のシステム構成内の小売店側装置の内部構成を示す図である。

【図5】図1のシステム構成内のクレジットカード会社の内部構成を示す図である。

【図6】図1のシステム構成内の運搬者側装置の内部構成を示す図である。

【図7】図1のシステム構成内の運搬者携帯装置の内部構成を示す図である。

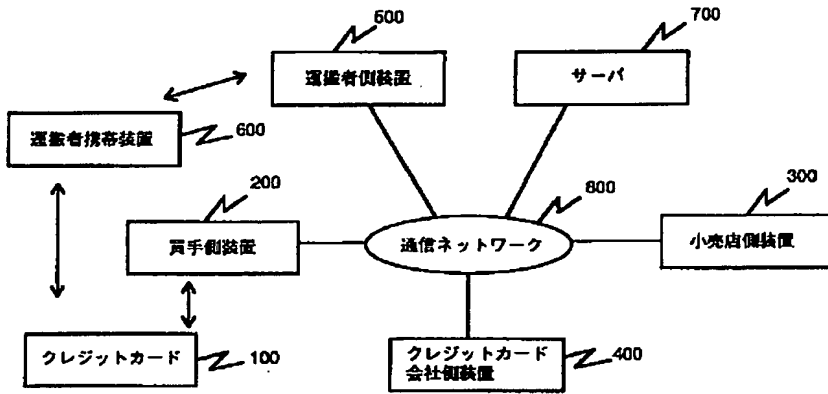
【図8】図1のシステム構成におけるショッピングの流れを示す図である。

【符号の説明】

100…クレジットカード、101…クレジットカード100内のメモリ、102…クレジットカード100内の署名作成装置、103…クレジットカード100内の暗復号化装置(公開鍵暗号)、200…買手側装置、201…買手側装置200内のクレジットカード読み取り装置、202…買手側装置200内の文書作成装置、203…買手側装置200内のハッシュ計算装置、204…買手側装置200内の暗復号化装置(共通鍵暗号)、205…買手側装置200内のメモリ、206…買手側装置200内の通信装置、300…小売店側装置、301…小売店側装置300内のハッシュ計算装置、302…小売店側装置300内の署名検証装置、303…小売店側装置300内の暗復号化装置(公開鍵暗号)、304…小売店側装置300内の鍵生成装置、305…小売店側装置300内の通信装置、400…クレジットカード会社側装置、401…クレジットカード会社側装置400内の署名検証装置、402…クレジットカード会社側装置400内のメモリ、500…運搬者側装置、501…運搬者側装置500内のメモリ、502…運搬者側装置500内の通信装置、503…運搬者側装置500内の暗復号化装置(共通鍵暗号)、600…運搬者携帯装置、601…運搬者携帯装置600内のクレジットカード読み取り装置、602…運搬者携帯装置600内のハッシュ計算装置、603…運搬者携帯装置600内の署名検証装置、604…運搬者携帯装置600内のメモリ、605…運搬者携帯装置600内の通信装置、606…運搬者携帯装置600内の表示装置、700…サーバ、800…通信ネットワーク。

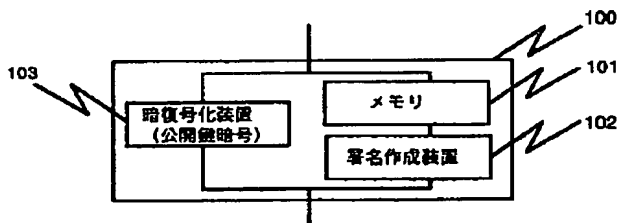
【図 1】

システム構成 (図 1)



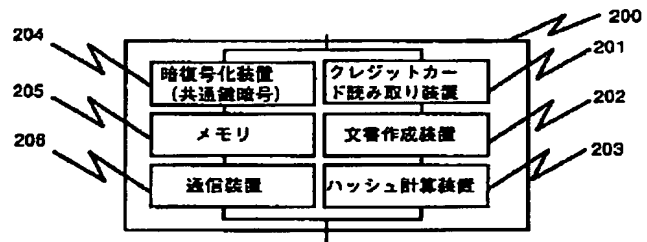
【図 2】

クレジットカード内部構成 (図 2)



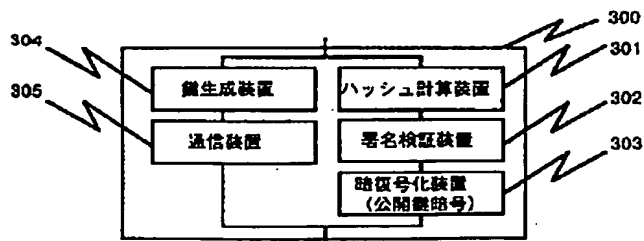
【図 3】

買手側装置内部構成 (図 3)



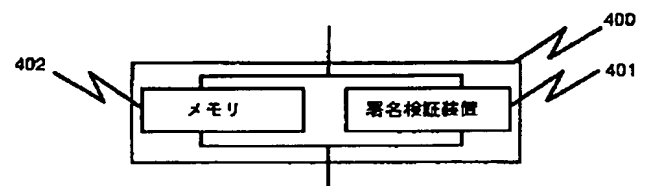
【図 4】

小売店側装置内部構成 (図 4)



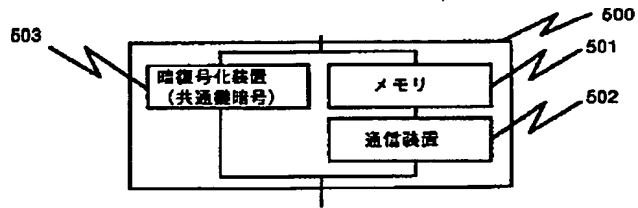
【図 5】

クレジットカード会社側装置内部構成 (図 5)



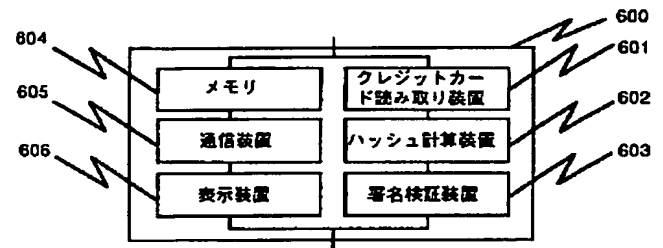
【図 6】

運搬者側装置内部構成 (図 6)

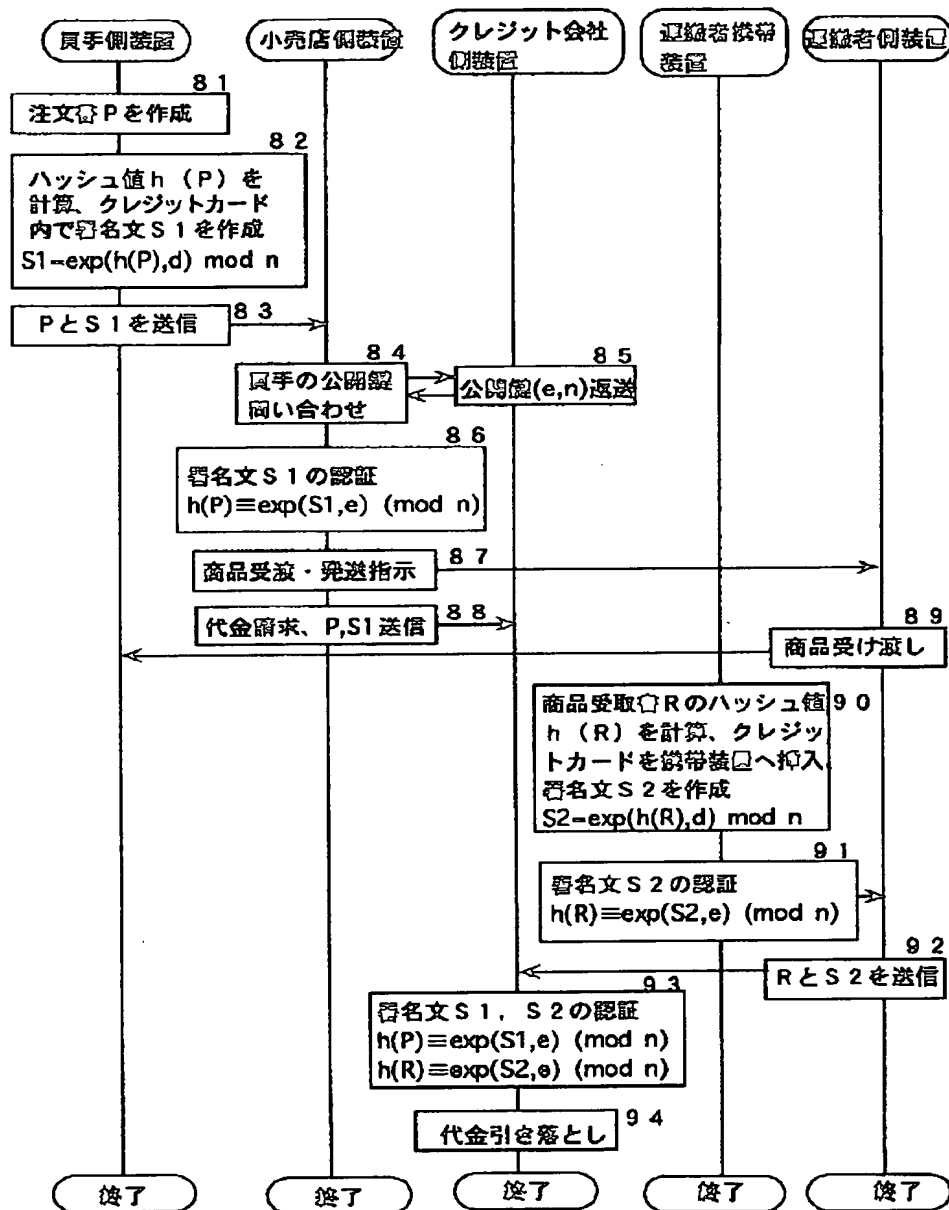


【図 7】

運搬者携帯装置内部構成 (図 7)



【図 8】



フロントページの続き

(51)Int.Cl.⁶

識別記号

庁内整理番号

F I

H 0 4 L 9/00

技術表示箇所

6 7 5 B

(72)発明者 梅木 久志
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 花岡 かほる
神奈川県川崎市幸区鹿島田890番地の12
株式会社日立製作所情報システム事業部内